Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б.Жильцов
«_11_» ____06_____ 2018 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «УНІВЕРСИТЕТСЬКІ СТУДІЇ: ВСТУП ДО СПЕЦІАЛЬНОСТІ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 0941/18
(підпис) (прізвище, ініціали)
«___» _____ 2018 р.

Київ – 2018

Розробник:

Бурячок Володимир Леонідович, доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладач:

Бурячок Володимир Леонідович, доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від ___.___.20___ р. № __

Завідувач кафедри _____ В.Л. Бурячок

(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Керівник освітньої програми _____ В.В. Семко

(підпис)

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ І.Ю. Мельник

(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___

(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___

(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___

(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___

(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
«Університетські студії»		
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	1	
Семестр	1	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	28	
Модульний контроль	8	
Семестровий контроль	-	
Самостійна робота	56	
Форма семестрового контролю	залік	
Змістовий модуль «Вступ до спеціальності»		
Курс	1	
Семестр	1	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	2	
Обсяг годин, в тому числі:	60	
Аудиторні	28	
Модульний контроль	4	
Семестровий контроль	-	
Самостійна робота	28	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Університетські студії: вступ до спеціальності» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчальних планів спеціальності 125 Кібербезпека.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Університетські студії: вступ до спеціальності» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Університетські студії: вступ до спеціальності» складається з двох змістових модулів: «Сучасні погляди на захист інформації в ІТСР», «Організація захисту об'єктів критичної інфраструктури». Обсяг дисципліни – 60 год (2 кредити).

Метою викладання навчальної дисципліни «Університетські студії: вступ до спеціальності» є студентам якісну теоретичну та практичну підготовку у вигляді знань, умінь та навичок за спеціальністю 125 Кібербезпека

Завдання:

– формування у студентів первинного уявлення про професію фахівця у галузі безпеки інформаційно-комунікаційних систем;

– формування у студентів впевненості у застосуванні одержаних знань на практиці.

У результаті вивчення навчальної дисципліни формуються такі компетентності:

– здатність до застосування знань у практичних ситуаціях;

– здатність до накопичення знань для розуміння предметної області та розуміння професії.

3. Результати навчання за дисципліною

При вивченні курсу «Університетські студії: вступ до спеціальності» студенти повинні бути здатними:

– здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій;

– застосовувати отримані знання, навички та практики щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур ОС тощо в професійній діяльності;

– вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

– проводити розслідування інцидентів інформаційної та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Сучасні погляди на захист інформації в ІТС							
***Тема 1*.** Загальні поняття про інформацію, інформаційний і кіберпростори, безпеку, події та інциденти безпеки	8	2	2				4
***Тема 2*.** Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу	10	2	2				6
Модульний контроль	2						
Разом	20	4	4				10
Змістовий модуль 2. Організація захисту об'єктів критичної інфраструктури							
***Тема 3*.** Тенденції впровадження сучасних цифрових технологій в системи безпеки критично важливих об'єктів інфраструктури. Поняття стратегії безпеки КВОІ	12	2	4				6
***Тема 4*.** Інтернет речей – як об'єкт критичної інфраструктури. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі	12	2	4				6
***Тема 5-6*.** Україна в умовах сучасних кіберзагроз: концептуальний підхід до формування систем інформаційної і кібербезпеки та захисту інформації	14	4	4				6
Модульний контроль	2						
Разом	40	8	12				18
Усього	60	12	16				28

5. Програма навчальної дисципліни

Змістовий модуль 1. Сучасні погляди на захист інформації в ІТС.
Основні питання:

- Ознаки інформаційної глобалізації. Форми та канали витоку інформації
- Поняття інфосфери, інформаційного та кіберпросторів.
- Загрози інформації в інформаційному і кіберпросторах та їх основні джерела.
- Загальні відомості про безпеку, події та інциденти безпеки.
- Поняття кібератаки. Приклади найбільш відомих атак на КВОІ
- Основні категорії та напрями здійснення кібкратак
- Методи, об'єкти впливу та суб'єкти здійснення кібератак
- Система протидії кібератакам.

Змістовий модуль 2. Організація захисту об'єктів критичної інфраструктури.
Основні питання:

- Тенденції розвитку світової цивілізації. Ключові цифрові тренди в Україні
- Ознаки об'єктів критично важливої інфраструктури та їх визначення
- Організація захисту КВОІ на прикладі АСУ ТП та можливі шляхи її вирішення
- Поняття цифрової стратегії безпеки КВОІ на прикладі АСУ ТП. Основні відмінності у формуванні й забезпеченні безпеки згідно Стратегії в бізнесі та критичній інфраструктурі
- Високорівневі рішення комплексної системи безпеки АСУ ТП КВОІ
- Інтернет речей як приклад реалізації об'єктів критично важливої інфраструктури
- Концепція реалізації та шляхи еволюції інтернету речей на період до 2020 року. Основні сегменти системи «Розумний дім» та організація їх взаємодії
- Слабкі місця Інтернету речей та його доля на ринку кібербезпеки

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	4	4
Відвідування семінарських занять	1	2	2	6	6
Відвідування практичних занять	1				
Відвідування лабораторних занять	1				
Робота на семінарському занятті	10	2	20	6	60
Робота на практичному занятті	10				
Лабораторна робота (в тому числі допуск, виконання, захист)	10				
Виконання завдань для самостійної роботи	5	1	5	2	10
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
	Разом	-	54	-	105
Максимальна кількість балів: 159					
Розрахунок коефіцієнта: 159/100=1,59					

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Сучасні погляди на захист інформації в ІТС		10	5
1	Моніторинг сучасних систем захисту інформації • виконання завдань відповідно до теми; • опрацювання фахових видань.	10	5
Змістовий модуль 2. Організація захисту об'єктів критичної інфраструктури		18	10
2	Сучасні технології захисту об'єктів критичної інфраструктури: • виконання завдань відповідно до теми; • опрацювання фахових видань.	18	10
	Разом	28	15

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для самоконтролю

1. Ознаки інформаційної глобалізації. Форми та канали витоку інформації
2. Поняття інфосфери, інформаційного та кіберпросторів.Їх загрози та уразливості
3. Загрози інформації в інформаційному і кіберпросторах та їх основні джерела.
4. Загальні відомості про безпеку, події та інциденти безпеки.
5. Поняття кібератаки. Приклади найбільш відомих атак на КВОІ
6. Категорії та напрями здійснення кібератак
7. Методи, об'єкти впливу та суб'єкти здійснення кібератак. Система протидії кібератакам.
9. Тенденції розвитку світової цивілізації. Ключові цифрові тренди в Україні
10. Ознаки об'єктів критично важливої інфраструктури та їх визначення
11. Організація захисту КВОІ на прикладі АСУ ТП та можливі шляхи її вирішення
12. Поняття цифрової стратегії безпеки КВОІ на прикладі АСУ ТП. Основні відмінності у формуванні й забезпеченні безпеки згідно Стратегії в бізнесі та критичній інфраструктурі
13. Високорівневі рішення комплексної системи безпеки АСУ ТП КВОІ
14. Інтернет речей як приклад реалізації об'єктів критично важливої інфраструктури
15. Концепція реалізації та шляхи еволюції інтернету речей на період до 2020 року. Основні сегменти системи «Розумний дім» та організація їх взаємодії
16. Слабкі місця Інтернету речей та його доля на ринку кібербезпеки

Шкала відповідності оцінок

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 60 год., лекції – 12 год., практичні заняття – 16 год., модульний контроль – 4 год., самостійна робота –28 год.

Модулі (назви, бали)	**Змістовий модуль 1.** Сучасні погляди на захист інформації в ІТС **(54 бали)**		**Змістовий модуль 2.** Організація захисту об'єктів критичної інфраструктури **(105 бали)**			
Лекції (теми, бали)	Загальні поняття про інформацію, інформаційний і кіберпростори, безпеку, події та інциденти безпеки (1 бал)	Структура та стислий опис сучасних кібератак. Загальні поняття про організацію захисту від їх деструктивного впливу (1 бал)	Тенденції впровадження сучасних цифрових технологій в системи безпеки критично важливих об'єктів інфраструктури. Поняття стратегії безпеки КВОІ (1 бал)	Інтернет речей – як об'єкт критичної інфраструктури. Тенденції розвитку та перспективи захисту IoT-пристроїв у світі (1 бал)	Україна в умовах сучасних кіберзагроз: концептуальний підхід до формування систем інформаційної і кібербезки та захисту інформації (2 бали)	
Практичні, семінарські заняття (теми, бали)	Поняття інфосфери, інформаційного та кіберпросторів. Їх загрози та уразливості (11 балів)	Кібератаки на КВОІ: категорії, напрями та методи здійснення (11 балів)	Тенденції розвитку світової цивілізації. Ключові цифрові тренди в Україні (22 бали)	Еволюція інтернету речей - концепція реалізації та шляхи здійснення (22 бали)	Україна на шляху до глобального Інформаційного суспільства (11 балів)	Заходи із забезпечення ІКБ в Україні та завдання силових структур (11 балів)
Самостійна робота	Самостійна робота (5 балів)		Самостійна робота (10 балів)			
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)			
Підсумковий контроль (вид, бали)	Залік					

8. Рекомендовані джерела

Основна (базова):

1. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. - К.: МОУ, 1999. - 456 с.
2. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.
3. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа /. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. – К. : ПВП «Задруга», 2014. – 320 с.
4. Прокофьев В. Ф. Тайное оружие информационной войны: атака на подсознание. Издание второе, расширенное и доработанное. Серия "Информационные войны". – М.: СИНТЕГ, 2003. - 408 с.
5. Почепцов Г.Г. Информационные войны.- М.: Рефл-бук, К.: Ваклер, 2001.- 576 с.
6. Гриняев С. Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. – Мн.: Харвест, 2004. – 448 с.
7. М.Левин. E-mail “безопасная”: взлом, “спам” и “хакерские” атаки на системы электронной почты Internet. – М.: Бук-пресс, 2006. – 192 с.
8. Peter Neumann. Computer-Related Risk. ACM Press/Addison Wesley, 1995.
9. Кузнєцов И.Н. Информация: сбор, защита, анализ. Учебник по информацион- но-аналитической работе. / И.Н. Кузнєцов. – М.: ООО Изд. Яуза, 2001. – 92 с.
10. Макнамара Д. Секреты компьютерного шпионажа. Тактика и контрмеры / Д. Макнамара; пер.с англ.; под ред. С.М. Молявко. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.

Додаткова

1. Перфильев Ю.Ю. Российское Интернет-пространство: развитие и структура / Перфильев Ю.Ю. - М.:Гардарики. 2003. - 272с.
2. Росич Ю.Ю. География развития Интернета в России: канд. геогр. наук / Росич Ю.Ю. - М., 2005. - 167с.
3. Богуш В.М. Основи інформаційної культури (електронний варіант). - К.: ДУІКТ, 2002. – 244 стор.
4. Грязнов Е.С., Панасенко С.А. Безопасность локальных сетей. – М.: Вузовский учебник, 2006.- 525 с.
5. Козлачков П.С. Основные направления развития систем информационной безопасности. – М.: финансы и статистика, 2004. – 736 с.
6. Леваков Г.Н. Анатомия информационной безопасности. – М.: ТК Велби, издательство Проспект, 2004. – 256 с.
7. Соколов Д.Н., Степанюк А.Д. Защита от компьютерного терроризма. – М.: БХВ-Петербург, Арлит, 2002. – 456 с.
8. Сыч О.С. Комплексная антивирусная защита локальной сети. – М.: финансы и статистика, 2006. – 736 с.
9. Швецова Н.Д. Системы технической безопасности: актуальные реалии. Спб: Питер, 2004. – 340 с.